

**DTS**

DanTech Services

Computers under control!™

Technology Times September 2018 Issue



Dan Foote
Owner/President

"As a business owner, I know you don't have time to waste on technical and operational issues. That's where we *shine!* Call us and put an end to your IT problems finally and forever!"

What's Inside:

Page 2

The Power Of Connection
by Marc Sanborn

Business Briefings:

- Why It's So Dangerous To Use
The Same Password For All Your
Online Accounts

- SECRET TECHNIQUES FOR
DEALING WITH LATE-PAYING
CLIENTS

Page 3

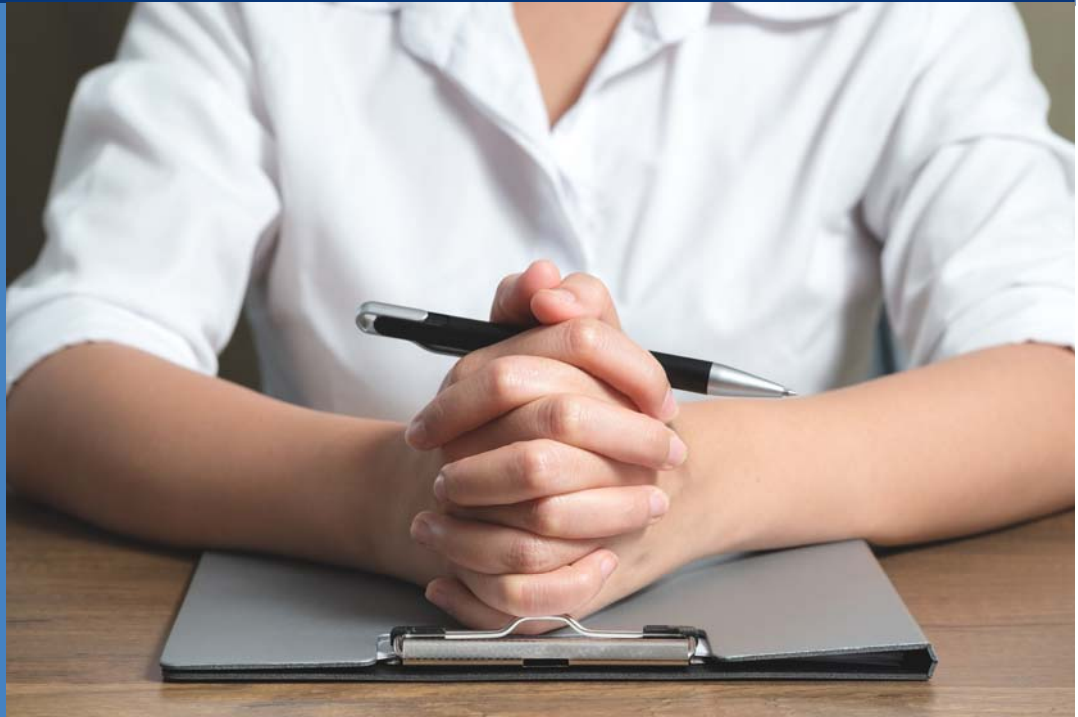
Protecting Your Business from
Cyber Tragedy

Layers of Protection

Page 4

Shiny New Gadget Of The Month:
Is This The Best Bag For
Frequent Flyers?

- "4 Questions You Should Ask Any
IT "Expert" Before Letting Them
Touch Your Network"
- Continued from page 1



4 Questions You Should Ask Any IT "Expert" Before Letting Them Touch Your Network

As businesses have become ever more dependent on technology, IT services providers have been popping up left and right. They've all got different strengths, capabilities and price points to consider. Some charge you by the hour and, while available to address any concerns you may have, they are pretty hands-off. Others are working on your network around the clock but charge more in turn. Many may boast an impressive record when working with a broad range of companies, but lack the experience necessary to understand the ins and outs of your specific industry. Some cost way too much month-to-month, while others try the "bargain bin" approach, but as a result, can't afford to field the staff needed to respond to issues in a timely fashion.

There's certainly a lot to consider when looking for an IT services provider for your business. And if you're not particularly knowledgeable about information technology yourself, it can sometimes feel like you're going into the process blind.

To suss out whether an IT company will mesh with your business's workflow and industry specific requirements, it's important to vet them thoroughly. The key is to ask the right questions. Here are four that will allow you to zero in on any IT company's priorities and strengths, and help you determine whether they're a good fit for your organization.

- Continued on page 4

Business Briefings:

Why It's So Dangerous To Use The Same Password For All Your Online Accounts

A complex password is a necessity in the age of cyberthreats, data breaches, and other security incidents. When you've landed on what you think is the perfect, complicated, yet easy-to-remember password, it's tempting to use it for every site you log in to. This is a shockingly common — and very dangerous — mistake.

When an online retailer or website gets hacked, oftentimes all you hear about in the news is how many credit card numbers were lost or the scope of the financial damage. You rarely hear about the thousands of user accounts that were compromised. But they're there!

If yours is among those compromised accounts, it's possible that your username and password are published and available to anybody who wants to look at it on the Internet. A clever crook knows that you probably use the same password on the compromised website as you do on your eBay, Amazon or other online accounts tied to your bank account. So, they try it out and, lo and behold, now they have access to your bank account.

It's possible to keep the password madness under control. Ask us for tips for having unique but memorable passwords. You might be surprised by how easy it really is.

SECRET TECHNIQUES FOR DEALING WITH LATE-PAYING CLIENTS

If you have a client who's habitually paying you late, it can be incredibly frustrating. But there are a few ways to mitigate the problem and get them back on track.

First, try billing twice per month or upfront instead of monthly. The former option will get them on a firm schedule and prevent getting backed up, while the latter will eliminate the problem altogether.

Also, try getting in touch with a contact in accounts payable. That way you can cut out the middleman and streamline the process.

Finally, make sure to send follow-up e-mails along with any invoice you send out. Pester them enough and they'll get the picture.

The Power Of Connection

By Marc Sanborn

Relationships are powerful. They help you differentiate your product or service, create brand loyalty, and set you apart from your competitors who are not willing to invest in building relationships.

Any savvy company will encourage its employees to build better relationships with customers. I myself teach the basics of relationship building in business, and have written about the process in my books, particularly *The Fred Factor*.

But you don't always have time to build a lasting relationship. Sometimes dealing with customers or clients only takes a few minutes and you have little to no contact with them later on. You don't have the time to build a "relationship," nor should you try.

But neither should you interact passively. There is something between a transaction and a relationship that will benefit both the customer and your business. The goal is to create a connection, which I define as a moment of shared affinity.

At a hotel in Miami, a bellhop who came to pick up a dry-cleaning order noticed I was wearing a Harley-Davidson T-shirt. "Do you ride?" he asked. That started a brief conversation about our shared interest in motorcycles. I saw him several times throughout my stay and felt a connection based on that brief exchange. We weren't friends by any definition, but the connection was still a positive part of my stay.

Transactions can be straightforward, but they often feel sterile. Looking for shared interests, indulging in appropriate humor, or simply noticing and commenting on another person is all it takes to add texture to the interaction and turn it into a genuine connection.

But how do you make these connections stronger?

1. Pay attention. Notice more about the person with whom you're interacting.
2. Look for similarities and points of contact.
3. Comment on what you find interesting.
4. Compliment on what you find praiseworthy.

Connecting in this way makes you more human and makes your business less sterile. Connecting with another person, even briefly, is always superior to simply completing a transaction.

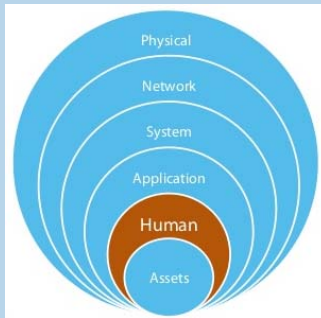
Facilitation Skills for Trainers

Two – Day Workshop
Mary M. Rydesky
Transition Management
2018
September 28 & October 1

Today, participants gain the most from time in class when trainers stop lecturing and start facilitating with techniques that make the information stick. *In other words, facilitating -- rather than training -- works with the new 'micro-learning' trend.*

Take your training activities to the next level by adding focused interactivity -
Sign up for *Facilitation Skills for Trainers* today.

Layers of Protection



Over the last 30 days, our Email Filtering service, CloudFilter aka MailStop, has handled about 78,000 emails. All, though, were not delivered. 33,400 were declared

spam, 3,670 were seen as an attack of some sort, over 1,000 contained a virus payload, and 126 were blocked by policy. This allowed us to deliver almost 40,000 hopefully legitimate emails. Yet we can almost always say that regardless of how effective our filtering services are, false positives and, worse yet, false negatives do occur.

A false positive would be an email that gets blocked when it should have been allowed. For whatever reason, it appears to be spam of some type. It's the false negatives that cause a greater concern. That's an email that gets delivered to the end user when it shouldn't. In the cat-n-mouse world of email filtering, the cat has to ever evolve to catch the metaphorical mouse that is actually spam, or worse yet, email that contains a malevolent payload. Or a link to a payload or web site that contains malware, ransomware, or is a very well-crafted phishing site.

Here's where a separate layer of protection, our Premium DNS service, steps in. Every click of a mouse creates a "call to action". Sometimes that action is "null", such as clicking on a blank space where no activity will occur. Sometimes a click will start an application, such as Word, Excel, Quick-Books or a web browser. Links in an email or on a web page cause another "call to action": a request to deliver content.

Good links take us to websites, portals and the data provided by that call to action or click of the mouse, allowing us to be productive and manage our businesses. Bad links that may sneak through our other filters would, if allowed, take us to websites, portals or payloads that can infect our PC's, turn them into unwitting bots, bitcoin generators, or ransom victims. Through our Premium DNS service, we have policies in place to prevent access to these malevolent sites.

Over that same 30 day span of time, we blocked almost 16,000 requests, prevented over 4,000 malware downloads and stopped 119 botnets out of over 25.3M requests. Taken in context, that's a very small percentage of the total requests yet all it takes is one click of a mouse to cripple a computer, network or business. These two layers of protection are key components of our services that are designed to keep your Computers Under Control, your networks, users and data safe, in a world full of IT risk.

#ProtectTheClick!

Protecting Your Business from Cyber Tragedy

Attacks on the Mat-Su, Valdez have companies scrambling for security
(This article was first published by Alaska Business Monitor on August 15, 2018)

By Dan Foote

A single click of the mouse can unleash catastrophic consequences to a business. Or a community. We've seen the recent headlines about what happened to one of our boroughs and another of our cities* "A multi-pronged, multi-vectored attack" most likely unleashed by a phishing email. Recovering from attacks such as these can be incredibly expensive. Witness Atlanta, Georgia and the millions of dollars spent to recover their systems (costs of up to \$17 million, reported as of August 6). One simple, single, solitary mouse click is all it takes.

The belief that your anti-virus program and firewall will protect you is a fallacy. Ignoring the cost of adequate protection also has a cost much higher than the monthly expense of securing a system and its users.

What does protection look like? While it depends on the organization, there are specific points of protection that should be mandatory. From an outside-in perspective, consider the following as minimum layers of protection:

- Email, spam, and virus protection
- Internet access with failover provisioning
- A commercial-grade firewall with active protection services
- Secure Wi-Fi with restricted access (if needed)
- Business Continuity—Disaster Recovery Data Protection (BCDR)
- Servers and PCs monitored and patched
- Modern anti-virus (yes, it's still needed)
- Premium DNS
- Appropriate policies for users
- User knowledge training

Not addressed yet are the higher level systems and security functions that add other layers, such as active monitoring of systems and services with more depth, adding privileged access management to a system, mobile device management and control, plus additional restrictions and controls that may be required for your industry for compliance purposes. Nor have we discussed protecting your cloud data, such as email delivered by Google or Office 365. These, too, can be an attack vector or target.

Arm chair quarterbacking is not the purpose of this piece. All of us in this industry know how fragile and tenuous security can be—even in high security instances. A single, well socially engineered piece of email or a web link that escapes detection can result in disaster—which is why we advocate multiple, overlapping layers of protection..

—[To read a full article please click here](#)



Visit our web-page at <https://www.dantechservices.com/infusionsoft/> to schedule a Demo Session!

Get More Free Tips, Tools, and Services at [https:// www.dantechservices.com](https://www.dantechservices.com)

Shiny New Gadget Of The Month:



Is This The Best Bag For Frequent Flyers?

If you're constantly travelling around the country for business, you need a piece of luggage that's essentially indestructible, and hopefully one that you can carry on any flight you need, saving on costs and precious minutes wasted at the luggage turnstile.

Luckily, with the Victorinox Lexicon Hardside Frequent Flyer 8-Wheel bag, you may have a contender that checks all your boxes. With a sleek, ergonomic, compact design, it offers plenty of volume without being bulky, along with a slick eight-wheel design that makes scooting around the ticket lines easier than ever. And for those of us living in the 21st century, there's a dedicated pocket for a battery pack, enabling you to attach a USB charging cord directly to your bag for when you need a little extra juice.

SONICWALL™

• SecureFirst •

*DanTech Services provides
knowledgeable management,
support & sales of*

SonicWALL UTM's.

Call 907-885-0500 to keep your
network secure
and your
Computers Under Control!™

- "4 Questions You Should Ask Any IT "Expert" Before Letting Them Touch Your Network"
- Continued from page 1

DO YOU TAKE A PROACTIVE OR 'BREAK-FIX' APPROACH TO IT?

When your car breaks down, you take it to the shop and you get it fixed. The mechanic charges you for the work done and for the parts, and then sends you on your way. Many business owners consider their computer network to be the same kind of deal. Why not just wait until an outage happens and then call up somebody who charges by the hour to fix it? That way, they imagine, they won't be paying for "extra" services they think they don't need.



But unfortunately, unlike your car, when your network is out, you're losing dollars every single minute. The cost of a network outage is difficult to overstate – not only will it bring your business to its knees while it's out, but it'll frustrate customers and employees and result in a cascading set of problems.

Instead of a "break-fix" technician on hand, you need a managed IT services provider. These experts work directly with your company to optimize your network and its security at every turn, and are available nearly any time to address your concerns. And they're genuinely invested in providing the best service possible, since it's in their best interest as well.

WHAT IS YOUR GUARANTEED RESPONSE TIME?

We've all needed something fixed before and had to wait for hours, days or even weeks before anyone bothered to come by and solve the problem. Don't let that happen to your business. If a company can't guarantee a response time, it's probably not a company you want to be working with.

WHAT WILL COST ME EXTRA?

This question is particularly important if you're looking at a managed services provider (which you should be). The last thing you need is for a crisis to strike, only to discover you need to shell out a bunch of surcharges to get your network back up and running. Make sure the costs and services included are crystal clear before you sign anything.

HOW MUCH EXPERIENCE DO YOU HAVE?

As scrappy as the "new kid on the block" may be, you don't want them in charge of one of the most important aspects of your business. Make sure any IT professionals you do business with have extensive experience not only in IT, but in your particular industry as well. That way they'll know exactly what to do to optimize processes and keep your data under lock and key.

